Transforming Legacy Systems To Obtain Information Superiority

Dr. David E. Corman, Thomas Herm, Dr. Kirby Keller, Charles Satterthwaite
{David.Corman, Thomas.Herm, Kirby.Keller}@MW.Boeing.com
The Boeing Company
P.O. Box 516 MC S270-4265
St. Louis, MO 63166-0516
{ Charles.Satterthwaite@wpafb.af.mil**}**
Air Force Research Laboratory
2241 Avionics Circle, Bldg. 620
Wright-Patterson AFB, OH 45433-7334

Abstract

The United States and its allies are being challenged by the advantages (and threats) of the Global Information Age. In response to these challenges, a new force structure is being proposed which is built upon global awareness, global engagement, and rapid deployment of specific (effects based) forces. Revolutionary advances in information resources and technology are key contributors to this force structure. In the face of a constrained DOD budget, an unprecedented system demand for lean operations in both peacetime and wartime, and the emergence of threats requiring immediate response, it is imperative that innovative technologies be developed to enable legacy weapon systems to exploit the information revolution, achieve information dominance, and meet the required operational tempo. This paper presents an embedded-system architecture, open system middleware services, and a software wrapper schema that will enable legacy systems to fully exploit evolving information technology capabilities in the context of an Network Centric Information Architecture (NCIA).

The Global Information Age

Current tactical environments are dominated by low bandwidth links and low capacity networks. Information available to the war-fighter is limited and often not timely. Advances in commercial Information Technology (broadband RF communications, wireless optical, fiber, optical switches, and routers) have the potential to enable new tactical architectures characterized by high-speed links and high capacity networks. Similarly, processor improvements, including optical processing, offer potential for increased automation and speed in handling and fusing of the available data to provide the right information to the war-fighter at the right time. Realizing this potential can be the decisive factor in battlefield success.

Concepts such as Dominant Battlespace Information are now seen as major contributors to warfighting success. The Joint Battlespace Infosphere (JBI) is being developed as a primary means to achieve information dominance by delivering the right information to the right user at the right time. The JBI may be viewed as the repository of all information that is digitally available to anyone regardless of format or media, location, classification level, or who owns it. This includes data in all knowledge bases, data warehouses, structured files, and text files. In addition to historic data, the JBI includes real-time data feeds provided by theater and national

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Transforming Legacy Systems to Obtain Information Superiority	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Lab,2241 Avionics Circle Bldg. 620,Wright-Patterson AFB,OH,45433-7334**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**9**	

intelligence and surveillance systems located in space, in the air, or on the ground. In the Air Force vision, weapon systems and the supporting command and control system elements can be considered nodes or IP addresses on a wide-area network. Through this wide-area network connectivity, the JBI can be accessed, searched, and manipulated to create new products. In other words, acting like nodes on the Internet, weapon and command and control systems are provided unparalleled on-demand access to a fused set of intelligence information provided by the collective set of tactical, theater, and national surveillance and intelligence systems - the JBI. Furthermore, the potential of each node to contribute to this collective situational awareness is fully enabled. Each node becomes both: 1) a server of raw data, collected by its on-board sensors and transmitted, to the JBI; and 2) a client of other information servers. Moreover, lines of demarcation between war-fighting and C2 nodes become less visible as discrete timelines for planning, execution, and assessment cycles merge.

The JBI cannot materialize out of thin air. Creating a "legacy-free" world of sensors, communication links, C3 systems, and weapon platforms is cost and risk prohibitive. The terminus of the information network – the embedded system / warfighting node - is our primary focus in this paper. It is here where the costs for a "legacy-free" infrastructure become truly staggering – much akin to the last few kilometers in the information network bringing broadband to the end-user. Evolutionary development, capturing and expanding the legacy embedded systems heritage, is the only viable migration path to connect legacy systems to the JBI. However, since most legacy weapon systems have been developed using point designs for connectivity, we must develop ways to "open them up" to take advantage of new technology and enable seamless information exchange.

This paper describes recent advances in "smart agent" technology that will enable "controlled" access to information optimized on a platform and mission basis. A key point here is the use of "information" as contrasted with data. We develop the concept of the "guardian agent" which serves as: 1) the link between the JBI and legacy embedded systems; 2) an integrator of tactical data into a coherent set of timely information; 3) a filter that works to manage the information flow to the warfighter based on information "pull"; and 4) an element of an information security strategy. This concept is central to distributed command and control, and flexible and timely employment of current weapon systems.

IEIST – Linking Legacy Systems to the JBI

The Insertion of Embedded Infosphere Support Technologies (IEIST) is an Air Force Research Laboratory initiative, being conducted with support from The Boeing Company. IEIST promises to deliver dramatic improvements in the exchange of information between deployed tactical elements including airborne C2 and information nodes

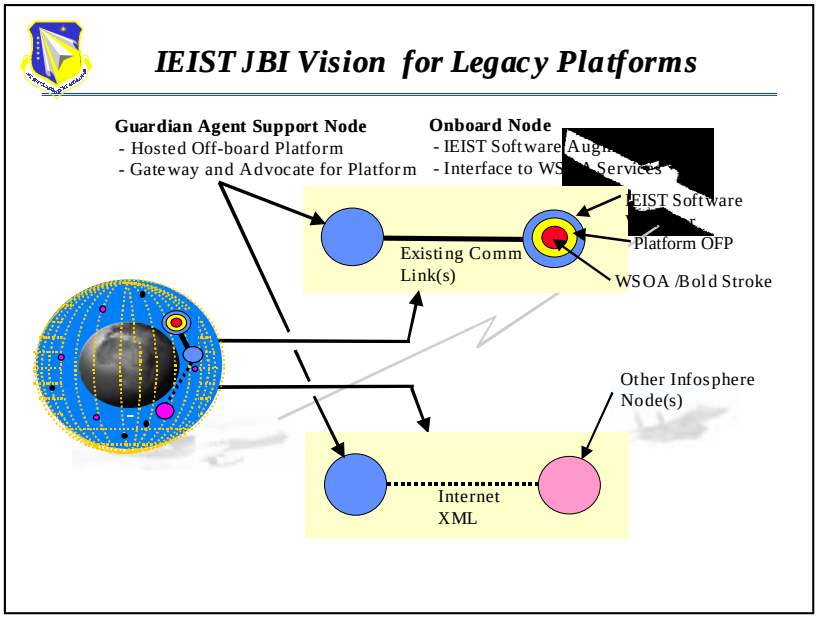

Figure 1. IEIST Guardian Agent Concept

world-wide. IEIST focuses on the development of off-board software agents, designed to augment embedded tactical systems and plug into the evolving JBI, whilst still providing interoperability with legacy systems and communication links, Figure 1. These Guardian Agent support nodes will be re-locatable anywhere within the JBI and will allow the use of readily available off-board processing and networking resources to augment the scarce embedded resources. Conservation of host resources - communications and processing bandwidth and operator effort – coupled with operational effectiveness will be the primary drivers in IEIST development. A small software object, the Host Agent, will be integrated into the host Operational Flight Program using proven software "wrapper" technologies in order to provide requisite communications back to the Guardian and to interface with the operator.

Figure 2 provides amplifying information on the key elements of an IEIST "Tactical Node". The "Tactical Node" refers to the augmented embedded system, i.e. the tactical embedded system plus the augmenting infrastructure, which enables the embedded system to become a full contributor to and consumer of JBI information. The figure shows that each tactical node includes a Guardian Agent (GA), a Tactical Communications Manager (including links), a Force Template (FT) and a Host Agent.

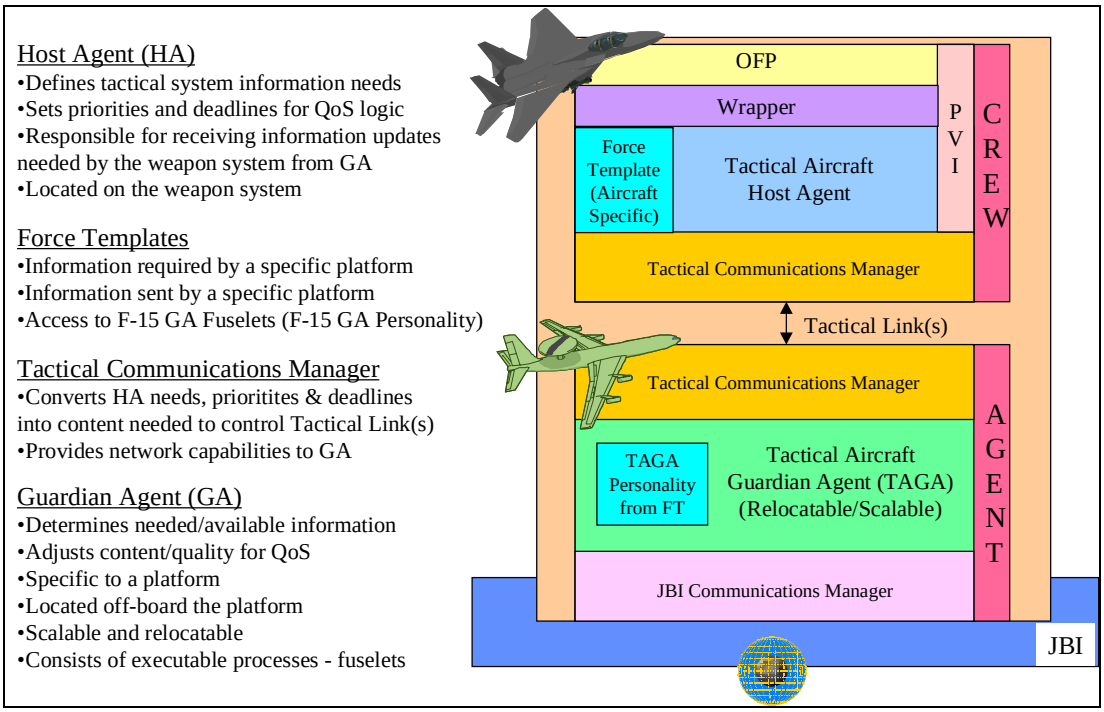

Figure 2. IEIST Program Elements

The GA identifies and accesses information of interest across the JBI, evaluates the tactical utility of the accessed information, and transmits the information to the tactical node using available communications. Similarly, the GA extracts information of interest from the tactical node and publishes it to interested elements across the JBI. It also brokers cooperative actions between its associated platform and other tactical nodes with specific focus on aiding the associated platform in establishing and executing cooperative actions with unmanned vehicles. This capability supports the controlled, but flexible and rapid, decision aiding/making among

tactical elements that is so important in the pursuit of Time Critical Targets. The GA is scaleable to the tactical need and relocatable anywhere within the JBI. It will be automated, requiring human intervention only in the most stressing tactical situations such as those in which potential for collateral damage is highest. In such critical scenarios, GA operation will be assigned to C2 elements where the requisite immediate asset allocation and airspace deconfliction decisions can be made. The GA design is generic in nature allowing reuse over a wide range of systems. The FT developed for each tactical system, contains a complete description of the information needs and generation capabilities of the tactical node. The FT will be used to tailor the GA to the specific requirements and capabilities of each tactical system.

Achieving information superiority must be considered within the context of an evolving information architecture that preserves legacy data links such as Link 16. Our GA design provides communications between the GA and all other JBI nodes through a CORBA interface with maximum reliance on XML message format for system flexibility and reuse. The CORBA interface lies above and is compatible with existing datalink layers. The Tactical Communications Manager (TCM) will utilize evolving quality of service (QoS) based delivery and data compression technologies to tailor information exchange to the tactical situation and available communications bandwidth through bandwidth monitoring and negotiation to optimize network availability.

The GA concept also includes use of emerging JBI services and fuselets that will tailor information capture and delivery to the mission needs. Prototype fuselets to be implemented in IEIST include: 1) Hierarchical Controller that provides automated re-allocation and optimization of strike assets based on real-time information updates; 2) Fusion Elements that provide smart filtering and integration of information, 3) Threat Evaluator that determines the impact of threat actions based on own-ship mission plans and vulnerabilities, and 4) Navigation and Discovery services for locating sources of information using CORBA services to match the right data producers and consumers. Figure 3 shows example JBI services under consideration for IEIST.

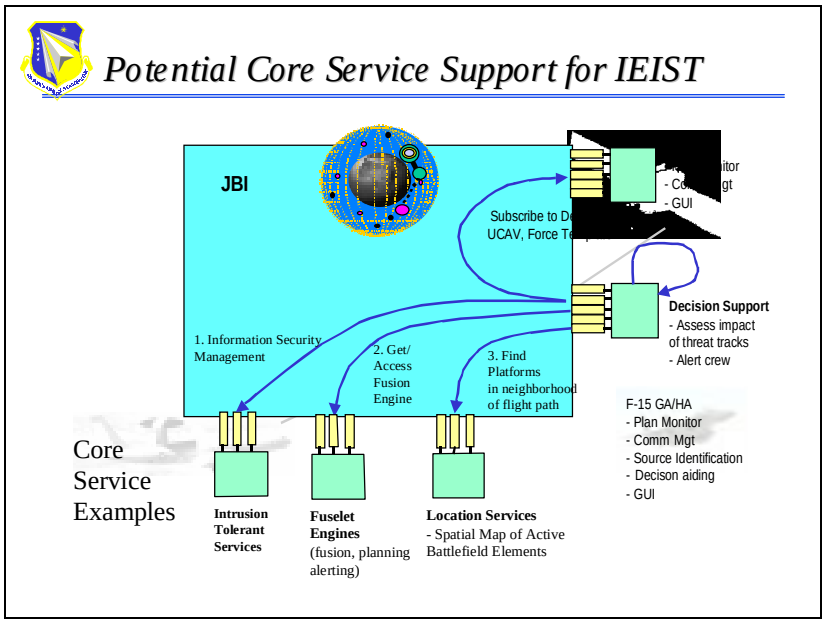

Figure 3. Example IEIST JBI Services

IEIST will also develop corresponding "Host Agent' capabilities for a number of tactical systems. The Host Agent is a relatively small software entity, which resides on the tactical node and operates in conjunction with the Operational Flight Software. The Host Agent will provide an interface between extant tactical system and the Guardian Agent, using legacy tactical data links for communications. It will include QoS logic similar to the Guardian Agent and will also satisfy any operator interface requirement associated with the additional IEIST functions. Host Agents for the F-15E, Unmanned Combat Air Vehicle (UCAV) and C2 node (airborne or ground based) are under development. Additional tactical systems may be added as the IEIST scenarios evolve.

IEIST responds to the critical need to concurrently evolve the JBI and embedded systems to ensure each responds to the specific needs of the other. Figure 4 graphically depicts this evolution in which IEIST Technologies, adapted to both legacy and emerging tactical systems through the specifics of their Force Templates, are being developed compatible with evolving JBI standards. These technologies will populate ground-based and airborne C2 elements located anywhere within the JBI. Through a series of demonstrations, IEIST will continue to increase the scope, fidelity and operational utilities of these technologies while concurrently developing a set of JBI service requirements. Early integration of IEIST into evolving JBI experiments and prototypes will ensure that embedded nodes and the JBI remain compatible and mutually beneficial and that those JBI services, most useful to tactical systems, will be developed fully responsive to tactical needs.

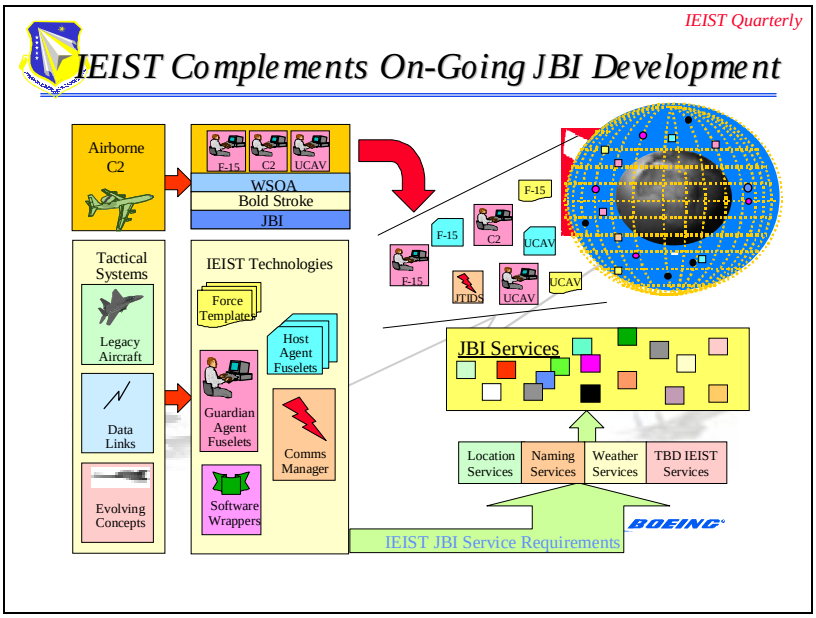

Figure 4. IEIST/JBI Evolution

As IEIST evolves, tactical decision aids and fuselets will be developed and tested in the IEIST context. Early emphasis is being given to basic capabilities such as Navigation and Discovery and Plan Monitor. Figure 5 shows the Navigation and Discovery process in which the Guardian Agent navigates the JBI in order to discover potential sources of information. In order to support

this functionality, each entity registers with the JBI when it becomes available and whenever it has a major change of state. For example, an ESM platform would initially register with the JBI and provide its planned mission and sensor coverage. As other "tactical" assets register, they would evaluate the ESM platform capabilities against their mission needs and if the ESM platform shows potential for supplying tactically significant information, the registering asset's GA would subscribe to the ESM platform. Subsequently, the GA would evaluate each sensor report from the ESM platform for impact to the host asset. Only those ESM reports, which are of significance to the tactical asset, would be passed on. In another example, the "tactical" assets might determine that the ESM platform coverage does not intersect their mission needs. Later the ESM asset might be re-positioned. It would register this re-positioning which would trigger a re-evaluation by each tactical assets resulting in revision of the ESM subscribers list. Clearly the methodology for Navigation and Discovery is one, which requires joint evolution between tactical assets and the JBI.

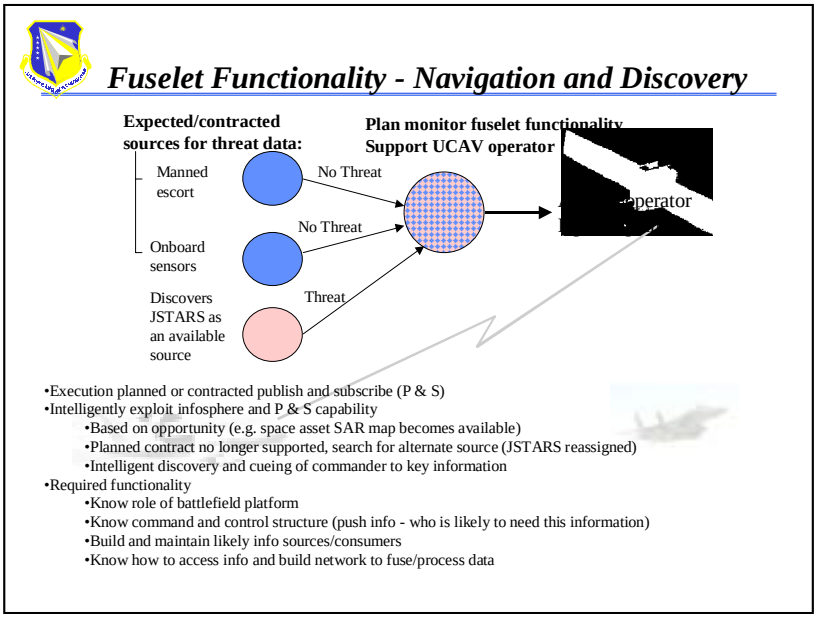

Figure 5. IEIST Navigation and Discovery

The majority of GA tasks center around the Plan Monitor, Figure 6. The GA continuously monitors the host flight status and plans and evaluates each item of information received from the JBI for its tactical significance. Continuing with the example in which the GA has subscribed to an ESM asset. Each time the ESM assets publishes a report, the GA evaluates it in a multi-step process. First, the GA calls upon a JBI service to identify the exact nature of the emission source, i.e. to identify the threat. The GA then compares the threat to the laydown, which was used to create the tactical plan. If the threat was known and was active at the time of plan generation, there is no new information contained in the ESM report and it is neglected. On the other hand, if the threat is new or

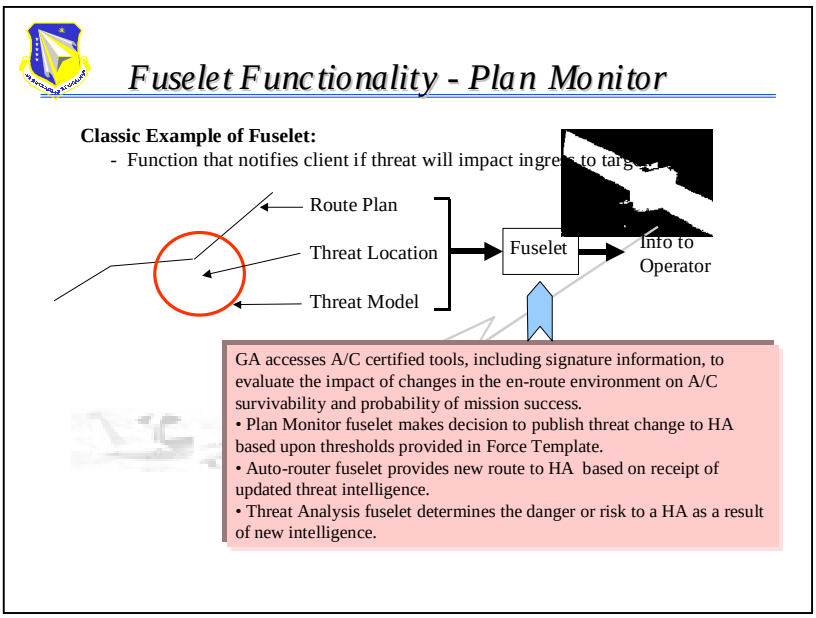

Figure 6. Plan Monitor

was thought to be inactive, it must be evaluated against the plan. If analysis of the threat indicates it poses a hazard to the host, the GA will take action to notify the host and either alter the plan or to eliminate the threat. In either case, additional decision aids and fuselets come into play either to replan the route or to negotiate for additional assets to neutralize the threat.

As IEIST progresses the number and fidelity of fuselets and decision aids will expand. In particular, the prosecution of Time Critical Targets poses a myriad of information exchange and real-time decision-making problems. Revolutionary advances are occurring in information technology that can automate and support real-time decision-making. While these have largely been targeted to commercial applications, they offer great promise for dramatic reductions in activity timelines, and improving the quality of real-time decision-making. As illustrated in Figure 7, under IEIST and other initiatives, Boeing is working to adapt techniques such as Common Object Request Broker Architecture (CORBA), adaptive middleware, and intelligent agents to legacy systems, particularly those that comprise the last parts of the "kill chain". The bottom right hand panel identifies specific technologies with greatest potential fit this problem area. These include software wrappers based on application of AFRL Incremental Upgrade for Legacy Systems (IULS) technology for gluing new applications to legacy systems, QoS based middleware to optimize use of networks and processors, and use of CORBA over Link 16 - in effect turning the link into an open system bridge for real-time collaborative planning by C2 and attack nodes.

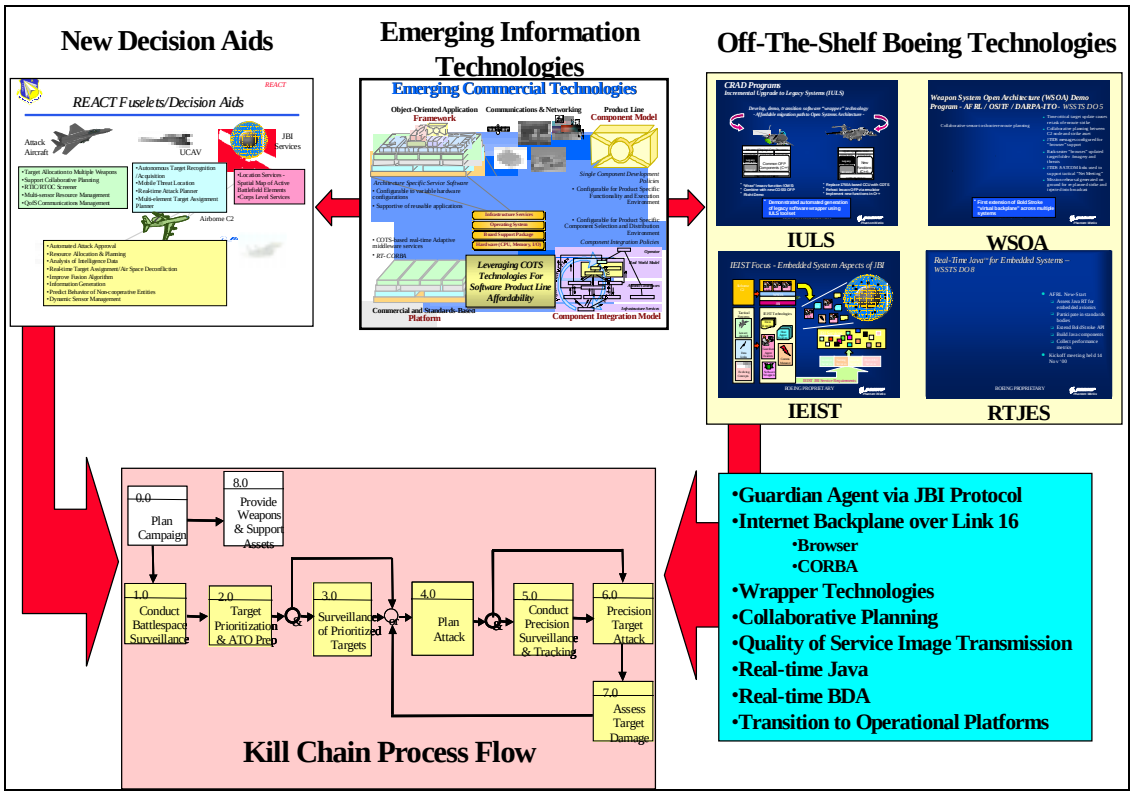

Figure 7. Shortening the TCT Kill Chain

Shortening the TCT Kill Chain will also require the capability to monitor and replan the mission in the aircraft or by an operator station. This requires the ability to: 1) Monitor elements of attack plan; 2) Support crew in awareness of the available ordnance, threat, targets and attack execution; 3) Provide mixed initiative interface to support crew/operator in editing, creating, and distributing plan adjustments; 4) Cue crew/operator recommendations/plan adjustments; 5) Provide means for crew/operator to empower unmanned vehicles to replan/react to changing conditions; and, 6) Provide automated replanning and execution capability that can interleave planning and execution in a dynamically changing environment. The intelligent agent paradigm is clearly applicable to this problem domain. Plan monitoring components will require capability to monitor the JBI to extract real-time status of assets within theater. IEIST Tactical Nodes will offer the opportunity to include legacy embedded systems in these evolving solutions.

Information assurance considerations may require IEIST components to be distributable and replicated at various air and ground nodes. Replication of GA components at multiple security domains is one technique to provide additional information security.

Summary and Conclusions

The IEIST effort began in April 2000 and continues through 2004. It will produce a series of laboratory demonstrations of increasing sophistication. Demonstrations focus on evolving IEIST technologies in the context of Network Centric Warfare and quantifying increases in operational capabilities. Initial efforts have been targeted at the first demonstration planned for September 2001. This demonstration will include a flight of F-15Es, and a squadron of UCAVs under the control of an airborne C2 node. The scenario includes: detection by the UCAVs of an emergent threat along the F-15 route, publication of the threat to the F-15s, evaluation of tactical alternatives by the F-15s, cooperative planning and neutralization of the threat by the UCAVs, transmission of UCAV Battle Damage Assessment to the F-15s and finally completion of the original mission objectives by the F-15s. All tactical communications will utilize a simulated Link 16 interface. Subsequent scenarios will incorporate more advanced war-fighting concepts with greater participation and decision making from the C2 node.

Progress to date includes development of the basic Guardian Agent and Host Agent designs, integration with battle-field level simulations and demonstration of a limited portion of the scenario. Substantial progress has also been made in defining prototype fuselets and identifying the impact of weapon system needs on NCW services.

References

[USAF, 1999] *United States Air Force Scientific Advisory Board Report on "Building the Joint Battlespace Infosphere"*, Volume 1: Summary, SAB-TR-99-02, December 17,1999.

[USAF, 1999] *United States Air Force Aerospace Command Control Intelligence, Reconnaissance (C2ISR) Campaign Plan 2000*, December 23, 1999.

[USAF, 1997] *Chairman of the Joint Chiefs of Staff, "Joint Vision 2010"*, May, 1997.

[USAF, 2000] *Chairman of the Joint Chiefs of Staff, "Joint Vision 2020"*, June, 2000.

Satterthwaite, C. P., Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid, 5th International Command and Control Research and Technology Symposium, Naval Post Graduate School, Monterey, CA., June 2000.